AN 2003-134037 [13] WPIDS

DNN N2003-106729 [13]

TI Apparatus authorization system e.g. for mobile telephone, attests wireless card based on certification information received from card, for operating mobile telephone

DC T01; W01

IN KAMAYA Y; NAKAKITA H

PA (TOKE-C) TOSHIBA KK

CYC 1

PI JP 2002366529 A 20021220 (200313)* JA 20[23]

ADT JP 2002366529 A JP 2001-171602 20010606

PRAI JP 2001-171602 20010606

IPCR G06F0015-00 [I,A]; G06F0015-00 [I,C]; G06F0021-20 [I,A]; G06F0021-20 [I,C]; H04L0009-32 [I,A]; H04L0009-32 [I,C]; H04Q0007-38 [I,A]; H04Q0007-38 [I,C]

AB JP 2002366529 A UPAB: 20050528

NOVELTY - Certification information for controlling operation of mobile telephone (20a), is generated by wireless card (10) and is transmitted to the mobile telephone. The mobile telephone is operated only when the card is attested based on the received certification information.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for apparatus certification method.

USE - For certifying wireless card to control operation of mobile telephone, PC, vehicle, etc., by user.

ADVANTAGE - Decoding of certification information by third person is prevented, hence safety of mobile telephone, PC, etc., is ensured.

DESCRIPTION OF DRAWINGS - The figure shows the structure of apparatus authorization system. (Drawing includes non-English language text).

Wireless card (10)

Mobile telephone (20a)

MC EPI: T01-J; W01-A05B; W01-B05A

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－366529
（P2002－366529A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｂ０８５
			３３０Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｋ０６７
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数10　ＯＬ　（全 20 頁）

(21)出願番号　特願2001－171602(P2001－171602)

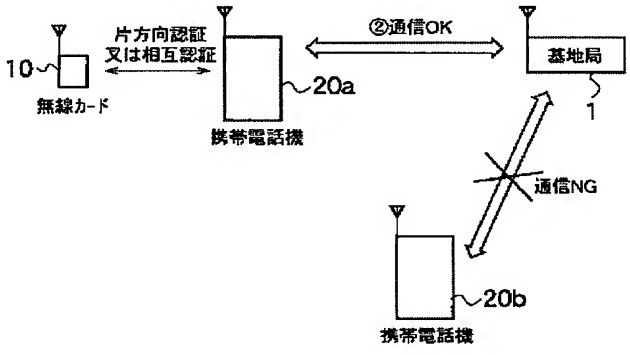
(22)出願日　平成13年６月６日(2001.6.6)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　中北　英明
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　釜谷　幸男
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　機器認証システム及び機器認証方法

(57)【要約】
【課題】　電子機器（例えば、携帯電話機２０）を使用する際に、利用者が所有する無線カード１０を用いて、その無線カード２０と電子機器との間で認証を行うことにより、その電子機器の使用を可能とするものである。
【解決手段】　電子機器（例えば、携帯電話機２０）の動作を制御するための認証を行う機器認証システムであって、電子機器の動作を制御するための認証情報を生成する第一認証部と、第一認証部で生成した認証情報を電子機器に送信する送信手段とを有する無線カード１０とを有し、電子機器は、認証情報を無線カード１０から受信する受信手段と、受信手段が受信した認証情報に基づいて無線カード１０の認証を行う第二認証部と、第二認証部の認証に基づいて電子機器を動作させる動作制御部とから概略構成される。



1

【特許請求の範囲】

【請求項１】　電子機器の動作を制御するための認証を行う機器認証システムであって、

前記電子機器の動作を制御するための認証情報を生成する第一認証部と、前記第一認証部で生成した認証情報を前記電子機器に送信する送信手段とを有する無線カードとを有し、

前記電子機器は、前記認証情報を前記無線カードから受信する受信手段と、前記受信手段が受信した前記認証情報に基づいて前記無線カードの認証を行う第二認証部と、前記第二認証部の認証に基づいて前記電子機器を動作させる動作制御部とを有することを特徴とする機器認証システム。

【請求項２】　請求項１に記載の機器認証システムであって、前記電子機器は、

前記認証情報を前記無線カードから取得するために、前記認証情報を要求する認証要求情報を生成する認証情報要求部と、

前記認証要求情報を前記無線カードに対して送信する送信手段とを有することを特徴とする機器認証システム。

【請求項３】　請求項２に記載の機器認証システムであって、前記電子機器は、

操作手段に対する操作を検知する検知部を有し、

前記認証情報要求部は、前記検知部での検知に基づいて、前記無線カードに対して前記認証情報を要求することを有することを特徴とする機器認証システム。

【請求項４】　請求項１又は請求項２に記載の機器認証システムであって、前記送信手段は、

前記受信手段に対して、前記受信手段と同じ通信条件を用いて、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信することを特徴とする機器認証システム。

【請求項５】　通信方式としてBLuetooth方式を使用したことを特徴とする請求項４に記載の機器認証システム。

【請求項６】　請求項２乃至請求項５に記載の機器認証システムであって、前記認証情報要求部は、前記認証要求情報を所定の時間毎に要求するようにするための要求時間を設定する設定手段を有することを特徴とする機器認証システム。

【請求項７】　電子機器の動作を制御するための認証を行う機器認証方法であって、

無線カードにおいて、前記電子機器の動作を制御する認証情報を生成し、その生成された前記認証情報を前記電子機器に送信するステップと、

前記電子機器において、前記無線カードから送信された認証情報を受信し、その受信した前記認証情報を認証し、その認証に基づいて前記電子機器を動作させるステップとを有することを特徴とする機器認証方法。

2

【請求項８】　請求項７に記載の機器認証方法であって、

前記電子機器において、前記認証情報を前記無線カードから受信するために、前記認証情報を要求する認証要求情報を前記無線カードに対して送信するステップと前記無線カードにおいて、前記認証要求情報を前記電子機器から受信し、その受信した前記認証要求情報に基づいて、前記認証情報を生成するステップとを有することを特徴とする機器認証方法。

【請求項９】　請求項８に記載の機器認証方法であって、

前記電子機器において、操作手段の操作を検知するステップと、その検知に基づいて前記認証要求情報を前記無線カードに対して送信するステップとを有することを特徴とする機器認証方法。

【請求項１０】　請求項８又は請求項９に記載の機器認証方法であって、前記電子機器において、

前記認証要求情報を所定の時間毎に要求するための時間を設定するステップと、　前記設定された時間に基づいて、前記無線カードに対して前記認証要求情報を送信するステップとを有することを特徴とする機器認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子機器の動作を制御するための認証を行う機器認証システム及び機器認証方法に関する。

【０００２】

【従来の技術】近年のＬＡＮ（Local Area Network）技術の発達に伴い、オフィス環境では、ＰＣ（Personal Computer）間の接続を中心として、ネットワーク化が進行している。また、有線ＬＡＮのみではなく、有線ＬＡＮの一部分を無線で置換する無線ＬＡＮ化も進んでいる。例えば、有線ＬＡＮに無線基地局を接続し、この無線基地局に複数のパーソナルコンピュータを無線で接続する無線ＬＡＮが挙げられる。即ち、基地局と携帯型ＰＣとの部分だけを見てみると、その部分は無線ＬＡＮを形成しているものである。この無線ＬＡＮを用いることは、伝送路として電波や赤外線などの無線通信技術を利用することになるので、配線敷設が不要となり、ネットワークの新設やレイアウト変更を容易に行うことができる。

【０００３】一方、このような無線通信技術の中でも特に注目されているのが、１０ｍ程度の近接距離のアドホックネットワークを構成することを対象としたBluetooth（以下、単に「BT」と略す）である。このBTは、通信速度が１ＭＢＰＳ程度、ＩｒＤａのような指向性はもたないなどの特徴がある。また、BTは、近い将来、１チップ５ドル程度という低コストで実現されようとしており、携帯電話業界、家電業界、更にＰＣ業界を巻き込ん

だ幅広い業種の約２０００社が標準化団体に参加している。そのため、BTを搭載した様々な無線機器が今後世界的に普及すると予想される。

【０００４】

【発明が解決しようとする課題】しかしながら、BTなどの無線機器は、ケーブル接続などの場合のように明示的な接続ではないので、セキュリティやプライバシーの保護が問題となりやすい。また、携帯性の高い機器は、落としやすいなどといった管理上の問題もあるので、前記機器を落としてしまった場合であっても、第三者に前記機器を使用できなくさせるようにするための方法が必要であった。

【０００５】そのため、従来から携帯電話機の場合には、図２３に示すように携帯電話機にパスワードを設定する機能を持たせており、他人に拾得され、又は、盗難されても、ある程度は携帯電話機を使用できなくさせることが可能であった。しかし、現実には、無線機器のユーザは、パスワード設定をあまり行っていないのが現状であり、また、パスワード設定がされていたとしても、銀行カードの場合のように、一旦パスワード設定すれば二度と変更する必要のないものとして一般的には認識されているものであった。

【０００６】したがって、パスワードを設定し、かつ、頻繁に変更している一般ユーザは、それほど多くはないものと考えられ、パスワード設定されていない携帯電話機が第三者に盗難等されてしまった場合には、第三者に不当な携帯電話機の使用がされる可能性があった。又、パスワード設定されていたとしても、パスワードの桁数が小さければ、総当たり攻撃などによってパスワードが簡単に破られてしまう恐れがある。

【０００７】そこで、本発明は以上の点に鑑みてなされたもので、電子機器を使用する際に、利用者の無線カードにより認証を行わなければ、その電子機器を使用することができないようにし、また、無線カード内にある特有の認証情報を、第三者に容易に解読させないようにするための機器認証システム及び機器認証方法を提供することを課題とする。

【０００８】

【課題を解決するための手段】本発明に係る発明は上記課題を解決すべくなされたものであり、請求項１に係る発明は、電子機器の動作を制御するための認証を行う機器認証システムであって、前記電子機器の動作を制御するための認証情報を生成する第一認証部と、前記第一認証部で生成した認証情報を前記電子機器に送信する送信手段とを有する無線カードとを有し、前記電子機器は、前記認証情報を前記無線カードから受信する受信手段と、前記受信手段が受信した前記認証情報に基づいて前記無線カードの認証を行う第二認証部と、前記第二認証部の認証に基づいて前記電子機器を動作させる動作制御部とを有することを特徴とするものである。

【０００９】このような請求項１に係る発明によれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を作動させることができる。そのため、電子機器で取得した認証情報が適正な情報でない場合には、前記電子機器を作動させることができず、適正な認証情報を持った者のみが電子機器を作動させることができる。

【００１０】また、電子機器は、無線カード（適正な認証情報が格納されたもの）を有する者のみしか使用できないことになるので、前記電子機器を盗難され、又は、紛失した場合であっても、その盗難した者等に使用させないようにすることができる。

【００１１】請求項２に係る発明は、請求項１に記載の機器認証システムであって、前記電子機器は、前記認証情報を前記無線カードから取得するために、前記認証情報を要求する認証要求情報を生成する認証情報要求部と、前記認証要求情報を前記無線カードに対して送信する送信手段とを有することを特徴とするものである。

【００１２】このような請求項２に係る発明によれば、電子機器の所有者は、電子機器を使用する際に、無線カードに対して電子機器を作動させるための認証情報を要求することができるので、電子機器の通信可能範囲内に無線カードがあれば、無線カードを持ち歩かなくても電子機器を作動させるための認証情報を無線カードから容易に取得することができる。

【００１３】請求項３に係る発明は、請求項２に記載の機器認証システムであって、前記電子機器は、操作手段に対する操作を検知する検知部を有し、前記認証情報要求部は、前記検知部での検知に基づいて、前記無線カードに対して前記認証情報を要求することを有することを特徴とするものである。

【００１４】このような請求項３に係る発明によれば、電子機器の利用者が電子機器を使用する際に、電子機器側の操作により無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カードと電子機器との間で認証を行うことができる。

【００１５】請求項４に係る発明は、請求項１又は請求項２に記載の機器認証システムであって、前記送信手段は、前記受信手段に対して、前記受信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信することを特徴とするものである。

【００１６】このような請求項４に係る発明によれば、送信手段は、受信手段に対して、その受信手段が有する特定の周波数とクロックのタイミングにより受信手段との間で通信接続を確立させることができるので、例えば、近接無線通信を行うＢＴ（Bluetooth）によって通信接続を確立させることができる。

【００１７】請求項５に係る発明は、通信方式としてBluetooth方式を使用したことを特徴とする請求項４に記載の機器認証システムである。

【００１８】このような請求項５に係る発明によれば、無線カードと電子機器との間の通信方式としてBluetooth方式を用いることができるので、通信速度が速く、相対的姿勢に自由度をもった通信をすることが可能となる。

【００１９】請求項６に係る発明は、請求項２乃至請求項５に記載の機器認証システムであって、前記認証情報要求部は、前記認証要求情報を所定の時間毎に要求するようにするための要求時間を設定する設定手段を有することを特徴とするものである。　このような請求項６に係る発明によれば、無線カードと電子機器との間の認証を所定の時間毎に行うので、無線カードを所持した利用者が電子機器から離れてしまい無線カードと電子機器との間で認証ができなくなった場合には、電子機器の動作を停止させることができる。そのため、第三者に電子機器のみが盗難された場合には、その盗難された電子機器と共通の認証情報を有する無線カードとの間で認証を行うことができないので、第三者に盗難された電子機器を不当に使用されることがなくなる。

請求項７に係る発明は、電子機器の動作を制御するための認証を行う機器認証方法であって、無線カードにおいて、前記電子機器の動作を制御する認証情報を生成し、その生成された前記認証情報を前記電子機器に送信するステップと、前記電子機器において、前記無線カードから送信された認証情報を受信し、その受信した前記認証情報を認証し、その認証に基づいて前記電子機器を動作させるステップとを有することを特徴とするものである。

【００２０】このような請求項７に係る発明によれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を作動させることができる。そのため、電子機器で取得した認証情報が適正な情報でない場合には、前記電子機器を作動させることができず、適正な認証情報を持った者のみが電子機器を作動させることができる。

【００２１】請求項８に係る発明は、請求項７に記載の機器認証方法であって、前記電子機器において、前記認証情報を前記無線カードから受信するために、前記認証情報を要求するための認証要求情報を前記無線カードに対して送信するステップと、前記無線カードにおいて、前記認証要求情報を前記電子機器から受信し、その受信した前記認証要求情報に基づいて、前記認証情報を生成するステップとを有することを特徴とするものである。

【００２２】このような請求項８に係る発明によれば、電子機器が無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カードと電子機器との間で認証を行うことができる。

【００２３】請求項９に係る発明は、請求項８に記載の機器認証方法であって、前記電子機器において、操作手段の操作を検知するステップと、その検知に基づいて前記認証要求情報を前記無線カードに対して送信するステップとを有することを特徴とするものである。

【００２４】このような請求項９に係る発明によれば、電子機器の利用者が電子機器を使用する際に、電子機器からの操作により無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カードと電子機器との間で認証を行うことができる。

【００２５】請求項１０は、請求項８又は請求項９に記載の機器認証方法であって、前記電子機器において、前記認証要求情報を所定の時間毎に要求するための時間を設定するステップと、前記設定された時間に基づいて、前記無線カードに対して前記認証要求情報を送信するステップとを有することを特徴とするものである。

【００２６】このような請求項１０に係る発明によれば、電子機器が無線カードに対して設定された時間毎に認証要求情報を要求することにより、無線カードと電子機器との間の認証を行うので、無線カードを所持した利用者が電子機器から離れてしまい無線カードと電子機器との間で認証ができなくなった場合には、電子機器の動作を停止させることができる。そのため、無線カードを所持している利用者が電子機器から離れている間は、第三者に電子機器を使用させないようにすることができる。

【００２７】

【発明の実施の形態】（機器認証システムの構成）本発明の実施形態について図面を参照しながら説明する。図１は、本実施形態に係る機器認証システムの概略構成図である。

【００２８】同図に示すように、本実施形態に係る機器認証システムは、主に、無線カード１０と携帯電話機２０ａとから構成されており、無線カード１０と携帯電話機２０ａとの間の認証が成功した場合にのみ携帯電話機２０ａを管理する基地局１と通信をすることができる。そのため、無線カード１０との間で認証が行われていない携帯電話機２０ｂは、基地局１と通信することができない。

【００２９】図２は、図１に示す無線カード１０と携帯電話機２０との間の認証方法を示したものである。同図に示すように、無線カード１０と携帯電話機２０には、両者に共通の秘密鍵SA１及び暗号アルゴリズムCA１が予め共有されている。例えば、この秘密鍵SA1及び暗号アルゴリズムは製造時に埋め込むことができる。

【００３０】無線カード１０には、乱数生成装置があり、乱数Ａを生成する。この乱数Ａは、無線カード１０から携帯電話機２０へと送信される。その乱数Ａなどを受信した携帯電話機２０は、秘密鍵SA１及び暗号アルゴ

リズムCA１によって暗号化する。そして、携帯電話機２０では、この暗号化された結果を応答として無線カード１０へと返信する。その後、無線カード１０側では、乱数Ａを秘密鍵SA1と暗号アルゴリズムCA1で暗号化したものを持ち、この応答と比較することによって認証の可否を判断する。この認証判断は、無線カード１０が携帯電話機２０の秘密鍵SA１及び暗号アルゴリズムCA１により認証判断するので、片方認証といわれる。尚、図２とは逆方向の片方認証もあり得る。

【００３１】図３は、無線カード１０と携帯電話機２０との間で行われる認証を相互から行ったことを示したものである。具体的には、同図に示すように、無線カード１０が携帯電話機２０の認証を行うだけでなく、携帯電話機２０の方からも無線カード１０の認証を行うものである。この無線カード１０と携帯電話機２０との間で相互の認証が成功し場合には、携帯電話機２０と基地局１との間で通信を行うことができる。

【００３２】これらの認証の確立は、操作性という面からはできるだけ短時間で終了するのが望ましい。また、このような認証用の無線カード１０は、携帯可能という点から、できるだけ小型で、且つ、普及を考えると低価格という要求条件がある。

【００３３】図４は、無線カード１０と携帯電話機２０との間で行われる認証を近接無線通信（本実施形態では、Bluetooth（以下単に「ＢＴ」と略す）を用いるものとする）を用いて認証したことを示したものである。具体的には、同図に示すように、先ず、製造時や出荷時などに、認証情報（PINコードなど）を管理しているホストシステム３０が両者に共通のPINコードを無線カード１０と携帯電話機２０に格納させる。その後、無線カード１０又は携帯電話機２０から両者に共通のPINコードや、乱数Ａ又は乱数Ｂを送信させることで、両者に共通の認証情報を生成させて、その生成させた認証情報に基づいて無線カード１０と携帯電話機２０との間で認証を行う（詳述は後述する）。

【００３４】そして、その認証が成功した場合には、携帯電話機２０と基地局１との間で通信を行うことができる。本実施形態では、無線カード１０と携帯電話機２０との認証は、ＢＴを用いて行うものとする。

【００３５】図５は、本実施形態に係る機器認証システムの内部構造を示すブロック図を示したものであり、本実施形態に係る機器認証システムは、ホストシステム３０と、無線カード１０、携帯電話機２０とを有している。

【００３６】前記ホストシステム３０は、無線カード１０又は携帯電話機２０を管理するものであり、パーソナルコンピュータ等が挙げられる。本実施形態では図５に示すように、ホストシステム３０内のシステム全体の制御を司るＣＰＵ３１と、ＣＰＵ３１が実行する制御プログラムを格納したＲＯＭ３２と、情報記録領域を備えたＲＡＭ３３と、無線カード１０との間で情報データの送受信をする通信Ｉ／Ｆ３４と、情報データの内容を表示させる表示部３７と、情報データを入力する操作部３６とを有している。

【００３７】このホストシステム３０は、無線カード１０及び携帯電話機２０を製造する際に、両者に共通のコード情報（例えば、PINコードなど）を無線カード１０にあるインターフェース（図示せず）（又は通信Ｉ／Ｆ３４）を介してＲＡＭ１３及びＲＡＭ２３に格納する（図５参照）。ここで、コード情報は、認証情報を生成させるための情報であり、本実施形態では、図６に示すように、任意に発生された乱数（１２８ビットのもの）、PINコード、PINコード長、暗証番号などが挙げられる。

【００３８】尚、ホストシステム３０は、例えば、工場内、又は、携帯電話機２０を販売している販売店、若しくは、代理店などに設置されているものである。従って、ホストシステム３０内でネットワークが構成されて、認証情報の分散管理がなされていればよい。

【００３９】表示部３７は、情報データを表示させる表示手段であり、例えば、液晶画面などが挙げられる。この情報データは、例えば、文字データ、画像データ、動画データ、コード情報、認証情報などが挙げられる。具体的に表示部３７は、ＣＰＵ３１からの命令により、記憶装置３５で格納されているコード情報を表示させるものである。また、表示部３７は、コード情報を通信Ｉ／Ｆ３４を介して無線カード１０に送信した場合には、表示部３７にある画面表示部に”コード情報は、○○○の無線カード１０に送信しました”などの表示をさせることもできる。

【００４０】操作部３６は、情報データを入力し、表示部３７にある画面表示を操作する操作手段であり、例えば、キーボードなどが挙げられる。尚、操作部３６の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【００４１】通信Ｉ／Ｆ３４は、無線カード１０又は携帯端末機２０との間で情報データの送受信をするものであり、例えば、BT、IrDA端末などが挙げられる。ここで、ＢＴとは、周波数ホッピング型のスペクトル拡散方式を用いてデータ通信を行うものである（詳しくは後述する）。また、IrDAとは、赤外線を利用してデータ通信を行うものである。

【００４２】記憶装置３５は、認証情報を格納するものであり、例えば、ハードディスク装置などが挙げられる。また、この記憶装置３５で蓄積するコード情報としては、ＰＩＮコードなどが挙げられる。具体的に記憶装置３５は、図７に示すように、携帯電話機２０毎に定められたＰＩＮ１～ＰＩＮｎを格納している。

【００４３】前記無線カード１０は、本実施形態では、電子機器の動作を制御するための認証情報を生成する第

一認証部と、第一認証部で生成した認証情報を電子機器に送信する送信手段とを有するものであり、本実施形態では同図に示すように、無線カード１０内のシステム全体の制御を司るＣＰＵ１１と、ＣＰＵ１１が実行する制御プログラムを格納したＲＯＭ１２と、無線カード１０と携帯端末機２０との間で認証を行うための認証情報を記録するコード情報領域１３ａを備えたＲＡＭ１３と、ホストシステム３０と携帯端末機２０との間で情報データの送受信をする通信Ｉ／Ｆ１４と、情報データの内容を表示させる表示部１５と、情報データを入力する操作部１６とを有している。

【００４４】尚、この無線カード１０の形状としては、カード状又はキーホルダー状のようなものが挙げられる。また、無線カード１０は、携帯電話機２０とセットで販売することができるものである。更に、無線カード１０は、携帯電話機２０と有線によって接続できるものであっても、また、携帯電話機２０のカードスロットに挿入する形式であってもよい。

【００４５】表示部１５は、情報データを表示させるものであり、例えば、液晶画面などが挙げられる。この情報データは、例えば、文字データ、画像データ、動画データなどが挙げられる。具体的に表示部１５は、ＣＰＵ１１からの命令により、通信Ｉ／Ｆ１４で受信した情報データを表示させるものである。例えば、無線カード１０と携帯電話機２０との間で適正な認証が行われた場合には、表示部１５は、ＣＰＵ１１からの命令により適正な認証が行われた旨の表示（例えば、”携帯電話機との認証は終了しました”。）をすることができる。

【００４６】操作部１６は、情報データを入力し、表示部１５にある画面表示を操作するものであり、例えば、キーボードなどが挙げられる。尚、操作部１６の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【００４７】ＲＡＭ１３は、電子機器の動作を制御するための認証情報を生成する第一認証部であり、本実施形態では、認証情報を生成するためのコード情報が格納されているコード情報記録領域１３ａを有している。このコード情報領域１３ａに格納されるコード情報としては、図６に示すように、１２８ビットで構成されている任意のコードである乱数、ＰＩＮコード（Personal Identification Number）、ＰＩＮコード長などが記録されている。このＰＩＮコードを記録する際には、外部から容易に書き替えられないようにした形式（プロテクターをかける）で格納することができる。

【００４８】このプロテクターをかけてＲＡＭ１３にＰＩＮコードを格納した場合に、その無線カード１０を紛失したときには、例えば、携帯電話機２０を製造工場又は販売店に持ち込んで、その製造工場又は販売店にあるホストシステム３０で以前格納してあったＰＩＮコードとは別のＰＩＮコードを設定する。これにより、無線カード１０を紛失したとしても、ＰＩＮコードを容易に書き替えることができないので、その紛失した携帯電話機２０を他の者によって使用させないようにすることができる。また、このとき、以前のＰＩＮコードは、ホストシステム３０で使用不可として管理可能である。

【００４９】一方、このＰＩＮコードは、無線カード１０の使用者が操作部１６を介して自由に設定させるようにすることもできる。例えば、無線カード１０の使用者が操作部１６でＰＩＮコードの長さを変更したり、又は、ＰＩＮコードを定期的に変更させたりすることができる。これにより、認証情報（ＰＩＮコードなど）を変更（定期的に）することができるので、無線カード１０と携帯電話機２０との間で行うデータ送受信の際のセキュリティレベルを自由に設定することができる。

【００５０】また、無線カード１０と携帯電話機２０との間でしか情報データを交信することができないようにするための秘密鍵（図示せず）や、操作部１６の操作により、暗証番号（例えば”１２３４”などの情報）も認証情報として用いることで、無線カード１０と携帯電話機２０との間でデータの送受信を行う際のセキュリティレベルを更に上げることができる。

【００５１】通信Ｉ／Ｆ１４は、ホストシステム３０と通信Ｉ／Ｆ１４との間で情報データの送受信をするものであり、例えば、BT、IrDAなどが挙げられる。本実施形態で通信Ｉ／Ｆ１４は、第一認証部で生成した認証情報を電子機器（例えば、携帯電話機２０）に送信する送信手段を有する送信部１４ａと、認証情報を要求するための認証要求情報を携帯電話機２０から受信する受信手段を有する受信部１４ｂと、無線カード１０で生成された認証情報と携帯電話機２０で生成された認証情報とが一致しているか否かを判断する認証部１４ｃとを有している。

【００５２】ＢＴの場合は、送信部１４ａは、受信手段（本実施形態では、携帯電話機２０の受信部２４ｂ）に対して、前記受信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に認証情報又は認証要求情報を送信する。

【００５３】このＢＴＩ／Ｆでは、通信可能な範囲内にある携帯電話機２０との接続可能性の向上等のために、待ち受け側のＢＴＩ／Ｆが接続要求を監視する周波数（待ち受け周波数）を所定時間毎に変化させている。

【００５４】この待ち受け周波数の変化パターンは、待ち受け側のＢＴＩ／Ｆに割り当てられた識別情報（ＢＴ-ＡＤ（Adress）、ＢＴ－ＣＬＫ（Clock））によって異なるが、通常、通信を開始しようとするときには、通信可能な範囲内に存在するＢＴＩ／Ｆの識別情報（特にＢＴ-ＡＤ）が不明である。このため、通信を開始しようとする送信部１４ａは、先ず、周囲のＢＴＩ／Ｆを検出するための問い合わせ（Inquiry）処理によって、自機

の周囲に存在するＢＴＩ／Ｆを検出する。

【００５５】このInquiryの要求に応じて、周囲のＢＴＩ／Ｆからの応答を受信部１４ｂが受信すると、この応答中のＢＴ－ＡＤに応じて通信しようとするBTを選択し、呼び出し(Page)処理によって、選択した相手を呼び出す。このPageにより、相手側のＢＴ送受信機が提供しているサービスを検出すると、所定のサービスを指定して、通信接続モードに移行し、接続を確立する。

【００５６】この無線カード１０と携帯電話機２０との間で通信接続が確立した後に、携帯電話機２０にある送信部２４ａ・受信部２４ｂと無線カード１０にある送信部１４ａ・受信部１４ｂとの間で認証情報が送受信されて、認証部１４ｃ及び認証部２４ｃで認証が行われる（詳細は後述する）。

【００５７】このＢＴを通信方式として用いることにより、鞄の中に無線カード１０を入れておいたり、又は、無線カード１０を携帯電話機２０に付けて携帯したりするというような利用形態で、無線カード１０と携帯電話機２０との間で簡単に認証処理をすることができる。そのため、無線カード１０を所有した者のみしか携帯電話機２０を使用することができなくなるので、携帯電話機２０を他の者によって許可なく使用されることがなくなり、携帯電話機２０を利用する際の安全性を高めることができる。

【００５８】認証部１４ｃは、無線カード１０で生成された認証情報と携帯電話機２０で生成された認証情報とが一致しているか否かを判断するものである。この認証部１４ｃで行う認証は、上述の如く、ＢＴで通信接続が確立された後に行われるものである。ここで認証情報としては、後述するリンクキーが挙げられる。

【００５９】この認証部１４ｃで行われる認証は、認証情報（リンクキー）によって定められる。ここでリンクキーとは、ある２つのＢＴＩ／Ｆ間において、１対１関係をセキュアに管理する共通パラメータのことをいうものである。

【００６０】セキュアに認証は、無線カード１０をマスター、携帯電話機２０をスレーブとして、ピコネットを形成してから行われ、この認証が成功したときのみ携帯電話機２０の使用が可能となる。ここでＢＴの認証情報（リンクキー）としては、初期化キーKin、単体キーＫａ、複合キーKabのいずれかが使用されるが、それぞれ１２８ビットの固有長を有する。

【００６１】以下、認証部１４ｃで行われるリンクキー（初期化キーKin、単体キーKa、複合キーKab）の生成と、そのリンクキーを用いて無線カード１０と携帯電話機２０との間で行われる認証について説明する。

【００６２】初期化キーKinの生成について図面を参照しながら説明する。図８は、初期化キーKinを生成するまでのブロック図を示したものである。また、図９は、初期化キーKinが生成されるまでの詳細なフロー図を示したものである。この初期化キーKinは、無線カード１０と携帯端末機２０とにあるＢＴＩ／Ｆ間で初めて接続を試みるときに使用されるリンクキーをいうものである。

【００６３】また、初期化キーKinは、後述する単体キーKa又は複合キーKabに置き換えられる一時的なキーではあるが、その単体キーKa又は複合キーKabが生成されるまでは初期化キーKinを保持しておき、認証の際に常に使用されるものである。

【００６４】図８に示すように、初期化キーKinの生成は、任意のコードである乱数１と、ＰＩＮ１と、ＰＩＮコード長とを、それぞれ無線カード１０と携帯電話機２０とにある認証部１４ｃ及び認証部２４ｃに入力させる。そして、認証部１４ｃ及び認証部２４ｃにある関数［Ｅ２２］は、入力された乱数１、ＰＩＮ１、ＰＩＮコード長とに基づいて初期化キーKinを生成させる。この関数［Ｅ２２］は、ＢＴＩ／Ｆに内蔵されているもので、初期化キーKinを生成するためのアルゴリズムを意味するものである。

【００６５】この初期化キーKinを生成するまでのフローについて図９を参照しながら説明する。同図に示すように、先ず、認証部１４ｃが、RAM１３からPIN１と、乱数１と、PINコード長とを読み込むことを行う（Ｓ１０１ａ）。一方、認証部２４ｃは、RAM２３からPIN1及びPINコード長を読み込むことを行う（Ｓ１０１ｂ）。

【００６６】そして、無線カード１０の送信部１４ａを介して、携帯電話機２０に乱数１を送信し、その送信された乱数１を携帯電話機２０で受信する（Ｓ１０２ａ、Ｓ１０２ｂ）。尚、無線カード１０及び携帯電話機２０に共通のPIN１は、無線カード１０と携帯電話機２０の製造工程でRAM１３及びRAM２３に予め格納しておく。

【００６７】その後、認証部１４ｃは、ＰＩＮ１と、ＰＩＮコード長、乱数１に基づいて初期化キーKinを関数［Ｅ２２］で生成させて（Ｓ１０３ａ）、その生成させた初期化キーKinをRAM１３に格納させる。

【００６８】一方、認証部２４ｃは、ＰＩＮ１と、ＰＩＮコード長と、無線カード１０から送信されてきた乱数１に基づいて関数［Ｅ２２］で初期化キーKinを生成させて（Ｓ１０３ｂ）、その生成させた初期化キーKinをRAM２３に格納させる。これにより、無線カード１０と携帯電話機２０との間で共通の初期化キーKinを所有させることができる。

【００６９】単体キーKaの生成について図面を参照しながら説明する。図１０は、単体キーKaを生成するまでのブロック図を示したものである。また、図１１は、単体キーKaを生成するまでの詳細なフロー図を示したものである。この単体キーKaは、ＢＴで恒久的に用いられるリンクキーをいうものであり、初期化キーKinを生成した後に生成されるものである。この単体キーKaにより、どのＢＴＩ／Ｆに対しても自分の単体キーKaをリンクキー

として用いることができるので、接続相手毎にリンクキーをデータベースで管理する必要がなくなる。

【００７０】図１０に示すように、無線カード１０側での単体キーKaの生成は、先ず、乱数２と無線カード１０のＢＴ－ＡＤ１とを認証部１４ｃに入力させる。そして認証部１４ｃにある関数［Ｅ２１］では、入力された乱数２と無線カード１０のＢＴ－ＡＤ１とを基に単体キーKaを生成させる。この関数［Ｅ２１］は、ＢＴＩ／Ｆに内蔵されているもので、単体キーKaを生成させるためのアルゴリズムを意味するものである。

【００７１】そして、関数［Ｅ２１］で生成させた単体キーKaは、初期化キーKinとの排他的論理和をして、その結果を携帯電話機２０へと送信する。その後、携帯電話機２０では、無線カード１０から送信された単体キーKaと初期化キーKinとの排他的論理和に、更に、携帯電話機２０で生成させた初期化キーKinとの排他的論理和をして単体キーKaを算出する。これにより、無線カード１０と携帯電話機２０との間で共通の単体キーKaを所有させることができる。

【００７２】この単体キーKaを生成させるためのフローについて図１１を参照しながら説明する。同図に示すように、先ず、認証部１４ｃ及び認証部２４ｃは、それぞれの無線カード１０及び携帯電話機２０にあるRAM１３及びRAM２３から初期化キーKin、乱数２及び無線カード１０のＢＴ－ＡＤを読み込む（Ｓ２１０ａ、Ｓ２０１ｂ）。尚、携帯電話機２０は、無線カード１０との間で行われる通信接続の段階で無線カード１０のＢＴ－ＡＤを既に取得している。

【００７３】そして、無線カード１０の認証部１４ｃが、乱数２と、無線カード１０のＢＴ－ＡＤとに基づいて関数［Ｅ２１］で単体キーKaを生成させる（Ｓ２０２ａ）。そして、その生成された単体キーKaと、予め無線カード１０が生成させた初期化キーKinとの排他的論理和（（Ka XOR Kin）；ここで”XOR”は排他的論理和を示すものとする（以下同様に扱う））を無線カード１０から携帯電話機２０へと送信する（Ｓ２０３ａ）。そして、認証部１４ｃで生成された単体キーKaは、RAM１３に格納させる（Ｓ２０４ａ）。

【００７４】一方、単体キーKaと初期化キーKinとの排他的論理和を無線カード１０から受信した携帯電話機２０は、その受信した単体キーKaと初期化キーKinと、携帯電話機２０側で生成させた初期化キーKinとの排他的論理和（（Ka XOR Kin）XOR Kin）をする。この排他的論理和（（Ka XOR Kin）XOR Kin）により、単体キーKaを算出させる。そして、その算出された単体キーKaはRAM２３に格納させる（Ｓ２０４ｂ）これにより、無線カード１０と携帯端末機２０との間で、共通の単体キーKaを保有させることができる。また、携帯電話機２０側では、乱数を発生させないで単体キーKaを生成させることができるので、認証が完了するまでの時間を幾分節約することができる。

【００７５】次に、複合キーKabの生成について図面を参照しながら説明する。図１２は、複合キーKabを生成するまでのブロック図を示したものである。図１３は、複合キーKabを生成するまでの詳細なフロー図を示したものである。この複合キーKabは、恒久的に用いるリンクキーであり、接続対象のＢＴＩ／Ｆが複数ある場合には、そのＢＴＩ／Ｆの数だけ存在するものである。

【００７６】また、初回の認証は、初期化キーKinによる認証を行うが、２回目以降は所定の条件を満たすことにより、単体キーKa又は複合キーKabによる認証を行う。この複合キーKabは、無線カード１０から生成させる単体キーKaと携帯電話機２０で生成させる単体キーKbとを共有させたものから構成される。

【００７７】図１２に示すように、無線カード１０で生成させる複合キーKabは、無線カード１０の単体キーKaを生成させる領域Ａ１と、携帯電話機２０の単体キーKbを生成させる領域Ａ４と、無線カード１０で発生させた乱数３と携帯電話機２０で発生させた乱数４とをそれぞれ交換させることを行う領域Ａ２及びＡ５と、無線カード１０と携帯電話機２０で各々複合キーKabを生成させる領域Ａ３及び領域Ａ６とから構成されるものである。

【００７８】この無線カード１０の単体キーKaを生成させる領域Ａ１では、先ず、無線カード１０で任意に発生させた乱数３と無線カード１０のＢＴ－ＡＤ１とを認証部１４ｃへと入力させる。そして、認証部１４ｃにある関数［Ｅ２１］は、乱数３と無線カード１０のＢＴ－ＡＤ１とに基づいて単体キーKaを生成させる。

【００７９】一方、携帯電話機２０の単体キーKbを生成させる領域Ａ４では、先ず、携帯電話機２０で任意に発生させた乱数４と携帯電話機２０のＢＴ－ＡＤ２とを認証部２４ｃへと入力させる。そして、認証部２４ｃにある関数［Ｅ２１］は、乱数４と携帯電話機２０のＢＴ－ＡＤ２とに基づいて単体キーKbを生成させる。

【００８０】また、領域Ａ２及び領域Ａ５では、無線カード１０で発生させた乱数３と、携帯電話機２０で発生させた乱数４とをそれぞれ交換させることを行う。この無線カード１０から携帯電話機２０へと乱数３を送信するときには、無線カード１０及び携帯端末機２０内で予め生成させておいた初期化キーKinと排他的論理和をとった後に携帯電話機２０へと送信させる。

【００８１】同様に、携帯電話機２０から無線カード１０へと乱数４を送信するときには、携帯電話機２０及び無線カード１０内で予め生成させておいた初期化キーKinとの排他的論理和をした後に無線カード１０へと送信する。このように無線カード１０と携帯電話機２０との間で発生する乱数３と乱数４とを交換する際に、初期化キーKinとの排他的論理和を行うのは、乱数３と乱数４とを送受信する際のセキュリティレベルを高めるためである。

【００８２】そして、領域Ａ２では、携帯電話機２０から送信された乱数４と初期化キーKinとの排他的倫理和に、無線カード１０で予め生成させておいた初期化キーKinとの排他的論理和を行い、乱数４を算出させる。一方、領域Ａ５では、無線カード１０から送信された乱数３と初期化キーKinとの排他的論理和に、携帯電話機２０で予め生成させておいた初期化キーKinとの排他的論理和を行い、乱数３を算出させる。

【００８３】また、無線カード１０で複合キーKabを生成させる領域Ａ３では、先ず、認証部１４ｃにある関数［２１］で、乱数４と携帯電話２０のＢＴ－ＡＤ２（携帯電話機２０との間で行われる通信接続の段階で既に受信）に基づいて携帯電話機２０の単体キーKbを生成させる。そして、関数［Ｅ２１］で生成された単体キーKbと、領域Ａ１で生成した単体キーKaとの排他的論理和をして複合キーKabを生成させる。

【００８４】一方、携帯電話機２０で複合キーKabを生成させる領域Ａ６では、認証部２４ｃにある関数［２１］で、乱数３と無線カード１０のＢＴ－ＡＤ１（無線カード１０との間で行われる通信接続の段階で受信）に基づいて無線カード１０の単体キーKaを生成させる。その後、その関数［Ｅ２１］で生成された単体キーKaと、領域Ａ４で生成させた単体キーKbとの排他的論理和により、複合キーKabを生成させる。

【００８５】この複合キーKabにより、片方認証（単体キーKaのみ）に比べて２倍のステップ数を行うので、より高いセキュリティレベルを確保することができる。

【００８６】複合キーKabを生成するまでの詳細なフローについて図１３を参照しながら説明する。同図に示すように、先ず、認証部１４ｃは、RAM１３から初期化キーKinと、乱数３と、無線カード１０のＢＴ－ＡＤ１とを読み込むことを行う（Ｓ３０１ａ）。一方、認証部２４ｃは、RAM２３から無線カード１０と同様の初期化キーKinと、乱数４と、携帯電話機２０のＢＴ－ＡＤ２とを読み込むことを行う（Ｓ３０１ｂ）。

【００８７】認証部１４ｃでは、無線カード１０のＢＴ－ＡＤ１と、乱数３に基づいて単体キーKaを関数［Ｅ２１］で生成させる（Ｓ３０２ａ）。一方、携帯電話機２０では、携帯電話機２０のＢＴ－ＡＤ２と、乱数４に基づいて単体キーKbを関数［Ｅ２１］で生成させる（Ｓ３０２ｂ）。

【００８８】無線カード１０は、予め所有している乱数３と初期化キーKinの排他的論理和をとり、その結果を携帯電話機２０に送信する（Ｓ３０３ａ）。そして、携帯電話機２０では、無線カード１０から受信した乱数３と初期化キーKinとの排他的論理和に、更に、携帯電話機２０が生成した初期化キーKinとの排他的論理和をして、乱数３を算出させる（Ｓ３０３ｂ、Ｓ３０４ｂ）。

【００８９】携帯電話機２０では、上記算出した乱数３と、無線カード１０のＢＴ－ＡＤ１とにより、無線カード１０と同様の単体キーKaを関数［Ｅ２１］で生成させる（Ｓ３０５ｂ）。そして、携帯電話機２０で予め所有している乱数４と初期化キーKinとの排他的論理和を携帯電話機２０から無線カード１０へと送信する（Ｓ３０６ｂ）。

【００９０】更に、無線カード１０では、携帯電話機２０から受信した乱数４と初期化キーKinとの排他的論理和に、無線カード１０で予め所有している初期化キーKinとの排他的論理和をして乱数４を算出させる（Ｓ３０４ａ、Ｓ３０５ａ）。そして、無線カード１０は、算出された乱数４と携帯電話機２０のＢＴ－ＡＤ２に基づいて単体キーKbを関数［Ｅ２１］で生成（Ｓ３０６ａ）させて、その生成された単体キーkbとＳ３０２ａで生成させた単体キーKaとの排他的論理和により複合キーKabを算出させる。その後、その算出された複合キーKabをRAM１３に格納させる（Ｓ３０８ａ）。

【００９１】一方、携帯電話機２０では、Ｓ３０２ｂとＳ３０５ｂとで生成された単体キーKaとKbとの排他的論理和をして、複合キーKabを算出させる（Ｓ３０７ｂ）。その後、その算出した複合キーKabをRAM２３に格納させる（Ｓ３０８ｂ）。これにより、無線カード１０と携帯電話機２０との間で複合キーKabを共有させることができる。

【００９２】上記リンクキーK（初期化キーKin、単体キーKa(Kb)、複合キーKab；以下これらを総称してリンクキーKとする）を用いて無線カード１０と携帯電話機２０との間で行われる認証について説明する。図１４は、無線カード１０と携帯電話機２０との間で行われる片方認証を示したブロック図である。

【００９３】同図に示すように、無線カード１０では、内部的に発生された任意の乱数５と、無線カード１０のＢＴ－ＡＤ１と、リンクキーKとを認証部１４ｃに入力させる。そして、認証部１４ｃにある関数［Ｅ１］は、入力された乱数５と、無線カード１０のＢＴ－ＡＤ１と、リンクキーKとに基づいて、ＳＲＥＳ（Signal Result）と呼ばれるパラメータを独立に算出する。

【００９４】一方、携帯電話機２０では、無線カード１０から乱数５を受信して、無線カード１０のＢＴ－ＡＤ１と、リンクキーKとを認証部２４ｃに入力させる。そして、認証部２４ｃにある関数［Ｅ１］は、入力された乱数５と、無線カード１０のＢＴ－ＡＤ１と、リンクキーKとに基づいて、ＳＲＥＳと呼ばれるパラメータを独立に算出する。そして、関数［Ｅ１］で算出されたＳＲＥＳのパラメータを無線カード１０へと送信する。

【００９５】尚、携帯電話機２０で所有される無線カード１０のＢＴ－ＡＤ１は、無線カード１０と携帯電話機２０との間で行われる問い合わせ（Inquiry）処理及び呼び出し（Page）処理により、既に取得しているものである。

【００９６】その後、認証部１４ｃでは、無線カード１

０で生成させたＳＲＥＳ’と携帯電話機２０で生成させたＳＲＥＳとを比較し一致しているか否かの認証を行う。そして、無線カード１０のＳＲＥＳ’と携帯電話機２０のＳＲＥＳが一致しているという判断をした場合には、無線カード１０から携帯電話機２０を動作させるための動作信号を送信し、その動作信号を受信した携帯電話機２０は、携帯電話機２０を稼働させる（詳述は後述する）。

【００９７】リンクキーKを用いて無線カード１０と携帯電話機２０との間で行われる片方認証の詳細なフローについて説明する。図１５は、無線カード１０と携帯電話機２０との間で行われる片方認証のフローについて示したものである。

【００９８】同図に示すように、先ず、認証部１４ｃ及び認証部２４ｃは、それぞれRAM１３及びRAM２３から初期化キーKinと、乱数５と、無線カード１０のＢＴ－ＡＤ１とを読み込むことを行う（Ｓ４０１ａ、４０１ｂ）。

【００９９】そして、無線カード１０は、無線カード１０の乱数５を携帯電話機２０へ送信する（Ｓ４０２ａ）。そして、無線カード１０から乱数５を受信した携帯電話機２０では、その受信した乱数５と、無線カード１０のＢＴ－ＡＤ１と、リンクキーKとに基づいてＳＲＥＳを関数［Ｅ２２］で生成させる（Ｓ４０２ｂ、Ｓ４０３ｂ）。そして、携帯電話機２０は、その生成されたＳＲＥＳを無線カード１０に送信する（Ｓ４０３ｂ）。

【０１００】その後、無線カード１０では、携帯電話機２０からＳＲＥＳを受信（Ｓ４０４ａ）し、その携帯電話機２０のＳＲＥＳと無線カード１０で生成したＳＲＥＳ’とを比較して両者が一致しているか否かの判断を行う（Ｓ４０５ａ）。そして、両者が一致している場合には、認証部１４ｃは、例えば、携帯電話機２０の動作を続行（又は始動）させるための動作信号を送信する（詳述は後述する）。

【０１０１】そして、その動作信号を無線カード１０から受信した携帯電話機２０は、受信した動作信号に基づいて携帯電話機２０を動作させる。又は、無線カード１０から動作信号を受信した携帯電話機２０は、無線カード１０から特定の登録情報（例えば、無線カード１０を所有している者の顔写真、氏名など）を受信し、表示部２５で表示さたりすることができる（詳述は後述する）。

【０１０２】リンクキーKを用いて無線カード１０と携帯電話機２０との間で行われる双方認証の詳細なフローについて説明する。図１６は、無線カード１０と携帯電話機２０との間で行われる双方認証のフローについて示したものである。

【０１０３】図１６に示すように、先ず、認証部１４ｃは、RAM１３からリンクキーKと、乱数５と、無線カード１０のＢＴ－ＡＤ１と、携帯電話機２０のＢＴ－ＡＤ２とを読み込む（Ｓ５０１ａ）。一方、認証部２４ｃは、RAM２３からリンクキーKと、乱数６と、無線カードのＢＴ－ＡＤ１と、携帯電話機２０のＢＴ－ＡＤ２とを読み込む（Ｓ５０１ｂ）。

【０１０４】そして、無線カード１０は、乱数５を携帯電話機２０へと送信する（Ｓ５０２ａ）。そして、無線カード１０から乱数５を受信した携帯電話機２０は、その受信した乱数５と、予め所有している無線カード１０のＢＴ－ＡＤ１と、予め算出しておいたリンクキーKに基づいてＳＲＥＳ１を関数［Ｅ２２］で生成させる（Ｓ５０２ｂ、Ｓ５０３ｂ）。

【０１０５】そして、携帯電話機２０は、関数［Ｅ２２］で生成されたＳＲＥＳ１を無線カード１０に送信する（Ｓ５０４ｂ）。一方、無線カード１０では、乱数５と、無線カード１０のＢＴ－ＡＤ１と、予め算出しておいたリンクキーKに基づいてＳＲＥＳ１’を関数［Ｅ２２］で生成させる（Ｓ５０３ａ）。

【０１０６】そして、無線カード１０は、無線カード１０で生成したＳＲＥＳ１’と、携帯電話機２０から受信したＳＲＥＳ１とが一致しているか否かを認証することを行う（Ｓ５０４ａ、Ｓ５０５ａ）。その無線カード１０で生成したＳＲＥＳ１’と携帯電話機２０で生成したＳＲＥＳ１とが一致していれば、認証が成功（認証成功１とする）したと判断して、次のステップに進むが、もし一致していなければ、無線カード１０と携帯電話機２０との認証が不成立として、次のステップには進めない。

【０１０７】その後、無線カード１０では、携帯電話機２０から乱数６を受信（Ｓ５０６ｂ）し、その受信した乱数６と、リンクキーKと、携帯電話機２０のＢＴ－ＡＤ２に基づいてＳＲＥＳ２’を関数［Ｅ２２］で生成させる（Ｓ５０７ａ）。そして、無線カード１０は、その生成されたＳＲＥＳ２’を携帯電話機２０へと送信する（Ｓ５０８ａ）。

【０１０８】一方、携帯電話機２０では、リンクキーKと、携帯電話機２０のＢＴ－ＡＤ２と、乱数６に基づいてＳＲＥＳ２をアルゴリズムＥ２２で生成させる（Ｓ５０６ｂ）。そして、携帯電話機２０は、無線カード１０からＳＲＥＳ２’を受信し、その受信したＳＲＥＳ２’と上記生成したＳＲＥＳ２とを比較して一致しているか否かを認証する（Ｓ５０７ｂ、Ｓ５０８ｂ）。そして、その携帯電話機２０で生成したＳＲＥＳ２と無線カード１０のＳＲＥＳ２’とが一致していれば、認証が成功（認証成功２とする）したと判断して、次のステップに進むが、もし一致していなければ、次のステップには進まない。

【０１０９】そして、無線カード１０と携帯電話機２０との上記認証が成功（認証成功１と認証成功２）した場合には、携帯電話機２０は、無線カード１０から登録情報などを受信する。

【０１１０】例えば、携帯電話機２０は、携帯電話機２０の操作を続行（又は始動）させるための続行信号を無線カード１０から受信し、その受信した続行信号に基づいて携帯電話機２０を作動（詳述は後述する）させて、登録情報などを無線カード１０から受信する。

【０１１１】前記携帯電話機２０は、認証情報に基づいて動作をする電子機器である。この電子機器は、携帯電話機のみならず、パーソナルコンピュータ、自動車なども対象として含まれるものとする。本実施形態で携帯電話機２０は、図５に示すように、携帯電話機２０内の全体の制御を司るＣＰＵ２１と、ＣＰＵ２１が実行する制御プログラムを格納したＲＯＭ２２と、無線カード１０と携帯端末機２０との間で認証を行うための認証情報を記録するコード情報領域２３ａを備えたＲＡＭ２３と、無線カード１０との間でデータの送受信をする通信Ｉ／Ｆ２４と、データの内容を表示させる表示部２５と、データを入力する操作部２６とを有しているものである。

【０１１２】表示部２５は、情報データを表示させる表示手段であり、例えば、液晶画面などが挙げられる。具体的に表示部２５は、ＣＰＵ２１からの命令により、通信Ｉ／Ｆ２４で受信した情報データを表示させる。また、無線カード１０と携帯電話機２０との間で適正な認証が行われた場合には、表示部２５では、適正な認証が行われた旨の表示（例えば、”無線カード１０との認証は終了しました”。）を行う。

【０１１３】操作部２６は、情報データを入力し、表示部２５にある画面表示を操作する操作手段であり、例えば、キーボードなどが挙げられる。尚、操作部２６の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【０１１４】ＲＡＭ２３は、無線カード１０と携帯端末機２０との間で認証を行うための認証情報を記録するコード情報領域２３ａを有するものである。このコード情報としては、１２８ビットで構成されている任意のコードである乱数、ＰＩＮコード（Personal Identification Number）、ＢＴ－ＡＤなどが挙げられる。

【０１１５】また、無線カード１０と携帯電話機２０との間でしか情報データを交信することができないようにするためｎ予め格納された秘密鍵のデータ（図示せず）や、操作部２６の入力操作による暗証番号（例えば”１２３４”などの情報）なども、コード情報として格納することができる。このコード情報により無線カード１０と携帯電話機２０との間で、ＢＴなどの通信方式によるものとは異なる認証処理を行うことができるので、無線カード１０と携帯電話機２０との間で行われるデータ送受信の際のセキュリティレベルを上げることができる。

【０１１６】前記ＣＰＵ２１は、携帯電話機２０内の全体の制御を司るものであり、本実施形態では、第二認証部の認証に基づいて電子機器を動作させる動作制御部２１ａと、操作手段に対する操作を検知する検知部２１ｂと、認証情報を無線カード１０から取得するために、認証情報を要求する認証要求情報を生成する認証情報要求部２１ｃとを有している。

【０１１７】動作制御部２１ａは、第二認証部（本実施形態では、認証部２４ｃ）の認証に基づいて電子機器（本実施形態では、携帯電話機２０）を動作させるものである。具体的に動作制御部２１ａは、認証部２４ｃにより、無線カード１０と携帯電話機２０との間の認証が成功した場合には、認証部２４ｃ（又は認証部１４ｃ）から携帯電話機２０の動作をさせるための動作信号が入力される。

【０１１８】動作信号が入力された動作制御部２１ａは、携帯電話機２０の動作を可能にするようにするために、携帯電話機２０の電源部２７にある電源を投入したり、又は、操作部２６を使用可能状態にする。尚、動作制御部２１ａは、電源部２７とは別の電源で動作するものであり、電源部２７が稼働していなくても動作制御部２１ａの動作が可能である。

【０１１９】検知部２１ｂは、操作部２６に対する操作を検知するものである。具体的に検知部２１ｂは、操作部２６の操作により発生された電流パルス、電圧パルスなどを検知するものである。そして、操作部２６の操作を検知した検知部２１ｂは、その検知した信号に基づいて、無線カード１０に対して認証情報を要求するための要求信号を認識情報要求部２１ｃへと出力させる。

【０１２０】認証情報要求部２１ｃは、認証情報を無線カード１０から取得するために、認証情報を要求する認証要求情報を生成するものである。具体的に認証情報要求部２１ｃは、検知部から要求信号が入力された場合には、無線カード１０に対して認証情報を要求するための認証要求情報を生成する。

【０１２１】そして、認証情報要求部２１ｃは、その生成した認証要求情報を送信部２４ａを介して無線カード１０へと送信させる。その後、認証要求情報を取得した無線カード１０は、認証部１４ｃで認証情報を生成させて、その生成した認証情報を携帯電話機２０へと送信し、その認証情報を受信した認証部２４ｃでは、受信した認証情報に基づいて認証を行う。

【０１２２】前記通信Ｉ／Ｆ２４は、無線カード１０にある通信Ｉ／Ｆ１４との間でデータの送受信をするものであり、例えば、BT、IrDAなどが挙げられる。本実施形態で通信Ｉ／Ｆ２４は、認証情報を要求する認証要求情報を無線カード１０に対して送信する送信手段を有する送信部２４ａと、認証情報などを無線カードから受信する受信手段を有する受信部２４ｂと、受信手段が無線カード１０から受信した認証情報に基づいて無線カード１０の認証を行う第二認証部を有する認証部２４ｃとを有している。

【０１２３】送信部２４ａは、受信手段（本実施形態では、無線カード１０の受信部１４ｂ）に対して、前記受

信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信する送信手段である。この送信部２４ａ－受信部１４ｂと送信部１４ａ－受信部２４ｂ間で行われる通信接続は、本実施形態では、BTを用いて行うものとする。

【０１２４】このBTは、通信可能な範囲内にある無線カード１０との接続可能性の向上等のために、待ち受け側のBTが接続要求を監視する周波数（待ち受け周波数）を所定時間毎に変化させている。

【０１２５】この待ち受け周波数の変化パターンは、待ち受け側のBTに割り当てられた識別情報（ＢＴ-ＡＤ（address）、ＢＴ－ＣＬＫ（Clock））によって異なるが、通常、通信を開始しようとするときには、通信可能な範囲内に存在するBTの識別情報（特にＢＴ-ＡＤ）が不明である。このため、通信を開始しようとする送信部２４ａは、先ず、周囲のBTを検出するための問い合わせ（Inquiry）処理によって、自機の周囲に存在するBTを検出する。

【０１２６】このInquiryの要求に応じて、周囲のBTからの応答を受信部２４ｂで受信すると、この応答中のＢＴ－ＡＤに応じて通信しようとするBTを選択し、呼び出し(Page)処理によって、選択した相手を呼び出す。このPageにより、相手側のＢＴ送受信機が提供しているサービスを検出すると、所定のサービスを指定して、通信接続モードに移行し、接続を確立する。

【０１２７】この通信接続では、無線カード１０と携帯電話機２０との間でデータのパケットの送受信は行われない。また、無線カード１０と携帯電話機２０との間で通信接続が確立した後に、携帯電話機２０にある送信部２４ａ・受信部２４ｂと無線カード１０にある送信部１４ａ・受信部１４ｂとの間で認証情報が送受信されて、認証部１４ｃ及び認証部２４ｃで認証が行われる。

【０１２８】認証部２４ｃは、無線カード１０で生成された認証情報と携帯電話機２０で生成された認証情報とが一致しているか否かを判断するものである。この認証部２４ｃで行う認証は、上述の通信Ｉ／Ｆ１４と同様に、無線カード１０との間で通信接続が確立された後に行われるものである。

【０１２９】この認証部２４ｃで行われる認証は、認証部１４ｃと同様の動作をするものであり、リンクキーという概念で管理されている。また、認証は、無線カード１０をマスター、携帯電話機２０をスレーブとして、ピコネットを形成してから行われ、この認証が成功したときのみ携帯電話機２０の使用が可能となる。

【０１３０】ここで用いられるＢＴのリンクキーとしては、主に初期化キーKin、単体キーＫａ、複合キーKabがあり、それぞれ１２８ビットの固有長を有する。このリンクキーの生成とそのリンクキーを用いた認証方法は、上記無線カード１０における認証部１４ｃと同様の方法で行われる（図８から図１６を参照）。

【０１３１】この認証部２４ｃでは、無線カード１０と携帯電話機２０との間の認証が成功したと判断した場合には、携帯電話機２０を動作させるための動作信号を動作制御部２１ａへと出力させる。また、認証部２４ｃは、無線カード１０の認証部１４ｃから通信Ｉ／Ｆ１４（２４）を介して携帯電話機２０を作動させるための動作信号を受け取ることもできる。

【０１３２】（機器認証システムを用いた機器認証方法）上記構成を有する機器認証システムによる機器認証方法は、以下の手順により実施することができる。図１７は、本実施形態に係る機器認証方法の手順を示すフロー図である。

【０１３３】同図に示すように、先ず、無線カード１０を使用したい携帯電話機２０に近づけるステップを行う（Ｓ６０１）。次いで、無線カード１０と携帯電話機２０との間の通信接続を確立させるステップと行う（Ｓ６０２）。具体的に、無線カード１０に複数の携帯電話機２０の認証情報が格納されている場合には、利用者が操作部１０を介して、使用したい携帯電話機２０の認証情報を選択し、その選択された認証情報に対応する携帯電話機２０と通信接続を行う。

【０１３４】次いで、無線カード１０と携帯電話機２０との間の認証を行う（Ｓ６０３）。具体的に、無線カード１０と携帯電話機２０との間で通信接続が確立した場合には、無線カード１０にある認証部１４ｄと携帯電話機２０にある認証部２４ｄとの間で、認証情報に基づいて上述した認証を行う。

【０１３５】次いで、無線カード１０と携帯電話機２０との間の認証が成功したか否かの判断を行うステップをする（Ｓ６０４）。具体的には、無線カード１０と携帯電話機２０との間で通信接続が確立した後に、無線カード１０にある認証部１４ｄと携帯電話機２０にある認証部２４ｄは、認証情報（初期化キーKin、単体キーKa、又は、複合キーKab）を各自生成させて、その認証情報により認証を行う。

【０１３６】また、この認証情報は、携帯電話機２０にある操作部２６の操作により認証情報を無線カード１０に対して要求することができる。具体的には、操作部２６の操作を検知部２１ｂが検知し、その操作部２６の操作を検知した検知部２１ｂは、その検知した信号に基づいて、無線カードに対して認証情報を要求するための要求信号を認識情報要求部２１ｃへと出力させる。

【０１３７】そして、認証情報要求部２１ｃは、検知部から要求信号が入力された場合には、認証情報を無線カード１０に対して要求するための認証要求情報を生成する。そして、送信部２４ａは、その生成した認証要求情報を無線カード１０へと送信させる。その後、認証要求情報を取得した認証部１４ｃは、認証情報を生成させ

て、その生成した認証情報を携帯電話機２０へと送信させる。その後、認証情報に基づいて、携帯電話機２０にある認証部２４ｃと無線カード１０にある認証部１４ｃで認証を行う（図８～図１６参照）。

【０１３８】次いで、無線カード１０と携帯電話機２０との間の認証が成功した場合には、携帯電話機２０を動作させるステップを行う（Ｓ６０５）。具体的には、無線カード１０にある認証部１４ｄと携帯電話機２０にある認証部２４ｄとの間で認証が成功したと判断した場合には、認証部１４ｄが携帯電話機２０の動作をさせるための続行信号を携帯電話機２０へと送信する。

【０１３９】そして、無線カード１０から動作信号を受信した通信Ｉ／Ｆ２４は、その動作信号を動作制御部２１ａへと入力させる。その後、通信Ｉ／Ｆ２４から動作信号が入力された動作制御部２１ａは、携帯電話機２０を動作させるために、電源部２７を稼働させて電源を投入させたり、又は、操作部２６を使用可能状態にする。

【０１４０】また、無線カード１０と携帯電話機２０との間で通信接続が確立され、認証が成功したときには、認証部２４ｃが携帯電話機２０を動作させるための続行信号を動作制御部２１ａへと出力させることもできる。一方、無線カード１０と携帯電話機２０との間の認証が成功しない場合には、携帯電話機２０を動作させないステップを行う（Ｓ６０６）。具体的には、無線カード１０にある認証部１４ｄと携帯電話機２０にある認証部２４ｄとの間で認証が成功しない場合（例えば、無線カード１０と携帯電話機２０とが遠く離れており通信できない場合には、認証できない）には、認証部１４ｄが携帯電話機２０の動作を続行させない（又は、始動停止）ようにするための動作拒否信号を携帯電話機２０へと送信する。そして、無線カード１０から続行拒否信号を受信した携帯電話機２０は、携帯電話機２０を続行させないようにするために電源の供給を切断したり、又は、操作部２６を使用不可状態にする。

【０１４１】その後、無線カード１０と携帯電話機２０との間の認証が成功したかの判断を行う（Ｓ６０７）。次いで、無線カード１０と携帯電話機２０との間で認証が成功した場合には、携帯電話機２０を操作させるステップを行う（Ｓ６０８）。これにより、無線カード１０を持った利用者が、携帯電話機２０の通信可能範囲内に入り再び無線カード１０と携帯電話機２０との間で認証処理を行った結果、この認証に成功すれば、携帯電話機２０を動作させることができる。

【０１４２】（機器認証システム及び機器認証方法による作用及び効果）このような本実施形態に係る機器認証システムによれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を作動させることができる。

【０１４３】そのため、電子機器で取得した認証情報が適正な情報でない場合には、前記電子機器を作動させないようにすることができ、適正な認証情報を持った者のみが電子機器を作動させることができる。また、電子機器は、無線カード（適正な認証情報が格納されたもの）を有する者のみしか使用できないことになるので、前記電子機器のみを盗難されたり、又は、紛失した場合であっても、その盗難した者等によって不当に使用されることがなくなる。

【０１４４】特に、本実施形態では、電子機器に操作部２６が設けられているので、その操作部２６を操作させることにより、無線カードに対して電子機器を作動させるための認証情報を要求することができる。そのため、電子機器の通信可能範囲内に無線カードがあれば、無線カードを持ち歩かなくても電子機器を作動させる認証情報を無線カードから容易に取得することができる。

【０１４５】また、送信手段は、受信手段に対して、その受信手段が有する特定の周波数とクロックのタイミングにより受信手段との間で通信接続を確立させることができるので、例えば、近接無線通信を行うＢＴを用いて認証を行うことができる。

【０１４６】また、本実施形態に係る機器認証方法によれば、電子機器は、無線カード側から電子機器を制御するための認証情報を取得することができるので、その認証情報に基づいて電子機器を動作させることができる。

【０１４７】（第１変更例）尚、本発明は上記実施形態に限定されるものではなく、本変更例では図１８に示すように、認証情報要求部２１ｃに認証要求情報を所定時間毎に要求するための時間を設定する設定部２１ｄと、設定部２１ｄで設定された時間を解除する解除部２１ｅとを設けてもよい。図１９は、本変更例１に係る機器認証システムの概略構成を示したものである。

【０１４８】同図に示すように、パーソナルコンピュータ２０にある設定部２１ｄで設定された時間毎に無線カード１０は、乱数７（又は乱数８）を送信し、その乱数７（又は乱数８）を送信したことによる応答１（又は応答２）をパーソナルコンピュータ２０から受信し、その受信した応答１（又は応答２）に基づいて認証を行い、パーソナルコンピュータ２０の動作の続行の可否を行うことを示したものである。

【０１４９】設定部２１ｄは、認証情報要求部２１ｃに認証要求情報を所定の時間毎に要求するための時間を設定する設定手段である。具体的には、利用者が操作部２６を用いて認証要求情報を要求する時間を設定し、その設定された時間信号を設定部２１ｄへと出力させる。

【０１５０】そして、操作部２６から時間信号が入力された設定部２１ｄは、その設定した時間が経過した場合には、無線カード１０と認証を行うようにするための認証命令信号を認証部２４ｃに出力する。そして、設定部２１ｄから認証命令信号が入力された認証部２４ｃは、無線カード１０との間で認証を行う。

【０１５１】解除部２１ｅは、設定部２１ｄで設定された要求時間を解除するものである。具体的には、利用者が操作部２６を用いて、設定された要求時間を解除するための操作をして、その要求時間を解除するための信号を解除部２１ｅへと出力させる。そして、その設定時間を解除するための信号が入力された解除部２１ｅは、設定部２１ｄで設定された要求時間を解除する。

【０１５２】上記構成を有する本変更例における認証の方法は、以下の手順により実施することができる（図示せず）。先ず、使用者がパーソナルコンピュータ２０の操作部１６を介して無線カード１０の認証を行う時間を設定するステップを行う。具体的には、利用者が、操作部２６の操作キーを入力してパーソナルコンピュータ２０が無線カード１０を定期的に認証する時間を設定し、その設定した信号（要求信号）を設定部２１ｄへと入力させる。

【０１５３】次いで、設定部２１ｂで設定された要求時間が経過した場合には、無線カード１０との間の認証を行うステップを行う。具体的に、操作部２６から要求信号が入力された設定部２１ｂは、その設定された要求時間が経過した場合には、無線カード１０と認証を行うようにするための認証命令信号を認証部２４ｃに出力する。そして、設定部２１ｄから認証命令信号が入力された認証部２４ｃは、無線カード１０との間の認証を行う。

【０１５４】その後、認証部２４ｃで無線カード１０との間で認証が成功したときには、パーソナルコンピュータ２０の使用を続行させるステップを行う。一方、認証部１４ｅでパーソナルコンピュータ２０との認証が失敗したときには、パーソナルコンピュータ２０の使用を続行させないステップを行う。

【０１５５】具体的に、認証部２４ｃで無線カード１０との間で認証が成功した場合には、認証部２４ｃは、パーソナルコンピュータ２０を続行させるための続行信号をに動作制御部２１ａに出力する。その続行信号が入力された動作制御部２１ａは、パーソナルコンピュータ２０をそのまま続行させる。

【０１５６】一方、認証部２４ｃは、無線カード１０との間で認証が成功しなかった場合には、パーソナルコンピュータ２０の動作を停止させるための続行拒否信号を動作制御部２１ａへと出力する。そして、続行拒否信号が認証部２４ｃから入力された動作制御部２１ａは、パーソナルコンピュータ２０の動作を続行させないようにするために、電源部２７にある電源を切断したり、又は、操作部２６で操作することができないようにする。

【０１５７】これにより、パーソナルコンピュータ２０は、無線カード１０を所持している利用者がパーソナルコンピュータ２０から遠ざかってしまい無線カード１０との間の認証に失敗したときには使用不可とさせることができる。そのため、無線カード１０を所持している利用者がパーソナルコンピュータ２０に近づいている時だけ、パーソナルコンピュータ２０を使用することができる。

【０１５８】また、無線カード１０を所持している利用者がパーソナルコンピュータ２０から離れてしまった場合には、パーソナルコンピュータ２０を稼働させないようにすることができるので、第３者に使用させないようにすることができる。そのため、パーソナルコンピュータ２０に格納されている情報の機密性を高めることができる。

【０１５９】（変更例２）また、複数の無線カード１０がある場合に、それらの無線カード１０が有する認証情報（ＢＴのＢＴ－ＡＤ(adress)、ＢＴ－ＣＬＫ(clock)、リンクキーKなど）を格納する統合手段（図示せず）を無線カード１０に設けてもよい。図２０は、本変更例における機器認証システムの概略構成図を示したものである。

【０１６０】同図に示すように、本変更例に係る機器認証システムは、無線カード１０ａ～１０ｃに対応する携帯電話機２０ａと、パーソナルコンピュータ２０ｂと、自動車２０ｃとに含まれる各認証情報（各機種のＢＴ－ＡＤ２０ａ～２０ｃ、リンクキーK1～K3）を１つの無線カード１０に統合したものである。

【０１６１】また、同図より、この無線カード１０を自動車（内部に設置されている機器も含む）のキーとしても用いることができる。これにより、無線カード１０とＢＴを搭載した自動車の組み合わせで、ドアの開閉や、エンジンの起動や、カーナビゲーションの操作をすることができる。この場合、無線カード１０を紛失したときには、先に述べたように、無線カード１０を販売店で再購入し、特定のＰＩＮコードなどを改めて設定することで、再びその自動車におけるキー（無線カード１０）又は免許証として用いることができる。

【０１６２】統合は、複数の無線カード１０が有する識別情報を格納することによって実現する。例えば、メモリカードなどが挙げられる。具体的に統合手段は、図２１に示すように、無線カード１０ｂの内部に存在するＳＤメモリカードインターフェース（図示せず）に他の無線カード１０ａ及び１０ｃを接続し、その接続した他の無線カード１０ａ及び１０ｃのＢＴ－ＡＤ２０ａ及び２０ｃとリンクキーK１及びK３とを格納する。

【０１６３】また、各無線カード１０が所有している識別情報をＢＴを介して統合手段に格納する場合には、例えば、無線カード１０ｂがマスターとなって、他の無線カード１０ａ及び１０ｃがスレーブとなるようなピコネットを形成させる。尚、このピコネットに属する無線カード１０ａ～１０ｃには、それぞれ異なったのＰＩＮコード（ＰＩＮ１～３）が設定されている。

【０１６４】そして、これらのＰＩＮ１～３をベースにして、マスターである無線カード１０ｂとスレーブであ

る無線カード１０ａ又は１０ｃとの間でそれぞれ通信接続を確立させ、マスターの無線カード１０ｂにある統合手段にスレーブの無線カード１０ａ又は１０ｃが有するそれぞれのＢＴ－ＡＤ、リンクキーKを格納させる。

【０１６５】これにより、複数の電子機器が有するそれぞれの認証情報（ＰＩＮコードなど）を１つの無線カード１０ｂが所有しているので、この無線カード１０ｂで複数の電子機器の動作を制御することができる。

【０１６６】無線カード１０は、１つの認証情報で複数の電子機器を制御するための情報を格納することもできる。例えば、図２２に示すように、無線カード１０に携帯電話機２０ａと、パーソナルコンピュータ２０ｂと、自動車２０ｃにそれぞれ同一のＰＩＮコードを設定する。そして、そのＰＩＮコードを無線カードにある統合手段に格納する。これにより、無線カード１０は、統合手段が所有しているＰＩＮコードと同一のＰＩＮコードを所有している電子機器の動作制御を行うことができる。尚、各無線カード１０が所有する識別情報の統合は、識別情報を管理するホストシステム３０で行うことができる。

【０１６７】これにより、携帯電話機２０ａと、パーソナルコンピュータ２０ｂと、自動車２０ｃに対応するそれぞれのＰＩＮコードを用意する必要がないので、製造工場で複数のＰＩＮコードを管理する必要がなくなる。

【０１６８】（変更例３）また、所定の時間帯において、無線カード１０に対して認証要求情報を要求する頻度を設定する時間帯設定部（図示せず）を通信Ｉ／Ｆ２１に設けてもよい。

【０１６９】時間帯設定部は、所定の時間帯において、無線カード１０に対して認証要求情報を要求する頻度を設定するものである。具体的には、先ず、利用者が操作部２６を操作させることにより、無線カード１０に対して認証要求情報を要求する特定の時間帯と、その特定の時間帯内で無線カード１０に対して認証要求情報を要求する回数を入力する。

【０１７０】例えば、電子機器２０の利用者が午前の１０時から１２時までの間に電子機器２０を使用する頻度が高ければ、利用者が所有する無線カード１０と電子機器２０との間の認証の回数（５分ごとなど）を多くし、一方、電子機器２０を利用する頻度が低い時間帯である午後７時から８時までの間は、電子機器２０と利用者が所有する無線カード１０との間で行う認証の回数を少なくする（１５分ごとなど）。

【０１７１】そして、操作部２６から認証情報を要求する特定の時間帯と、その特定の時間帯内で無線カード１０に対して認証情報を要求する回数が入力された時間帯設定部は、その設定された特定の時間帯と、その特定の時間帯内で無線カード１０に対して要求する回数とに基づいて、認証情報を要求するための要求信号を認証情報要求部２１ｃに出力する。

【０１７２】そして、時間設定部から要求信号が入力された認証情報要求部２１ｃは、認証情報を要求するための認証要求情報を生成し、その生成された認証要求情報を無線カード１０に対して送信する。その後、携帯電話機２０から認証要求情報を無線カード１０は、認証部１４ｃで認証情報を生成させて、その生成された認証情報により無線カード１０と携帯電話機２０との間で認証を行う。そして、無線カード１０と電子機器２０との間で認証が成功した場合には、電気機器２０の使用が可能となる。

【０１７３】これにより、時間帯設定部で設定された時間帯で電子機器２０と無線カード１０との間の認証を行う頻度を設定することができるので、電子機器２０を使用する頻度の高い時間帯に、電子機器２０と無線カード１０との間で認証を行う回数を多くすることができる。

【０１７４】そのため、電子機器２０を使用する頻度の高い時間帯には、電子機器２０と無線カード１０との間の認証を通常よりも多く行うことができるので、無線カード１０を所持する利用者が電子機器２０から少しの間離れたとしても、その間の電子機器の動作を停止することができ、電子機器２０に格納されている情報を第三者に盗用されることがなくなる。

【０１７５】

【発明の効果】以上説明したように本発明の機器認証システム及び機器認証方法によれば、電子機器を使用する際に、利用者の無線カードにより認証を行わなければ、その電子機器を使用することができないので、ユーザの電子機器（例えば、携帯端末機）が盗難等されたとしても第三者に不正に使用されることがなくなる。また、無線カード内にある特有の認証情報により認証を行うので、第三者に容易に認証情報を解読させないようにすることができる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る機器認証システムの概略構成を示すブロック図である。

【図２】本実施形態における無線カードと携帯電話機との間で行われる片方向認証を示した図である。

【図３】本実施形態における無線カードと携帯電話機との間で行われる相互認証を示した図である。

【図４】本実施形態における無線カードと携帯電話機との間の認証をＢＴを用いて行ったことを示した図である。

【図５】本実施形態における機器認証システムの内部構成を示したブロック図である。

【図６】本実施形態における無線カードと携帯電話機との間の認証で用いられるコード情報を示したものである。

【図７】本実施形態におけるホストシステムで管理されている携帯電話機のＰＩＮコードを示したものである。

【図８】本実施形態における無線カードと携帯電話機と

の間で認証する際に用いられる初期化キーKinが生成されるまでのブロック図を示したものである。

【図９】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる初期化キーKinが生成されるまでの過程を示したフロー図である。

【図１０】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる単体キーKaが生成されるまでのブロック図を示したものである。

【図１１】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる単体キーKaが生成されるまでの過程を示したフロー図である。

【図１２】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる複合キーKabが生成されるまでのブロック図を示したものである。

【図１３】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる複合キーKabが生成されるまでの過程を示したフロー図である。

【図１４】本実施形態における無線カードと携帯電話機との間で行われる片方認証を示したブロック図である。

【図１５】本実施形態における無線カードと携帯電話機との間で行われる片方認証を示したフロー図である。

【図１６】本実施形態における無線カードと携帯電話機との間で行われる相互認証を示したフロー図である。

【図１７】本実施形態における機器認証方法を示したフロー図である。

【図１８】第１変更例に係る機器認証システムの概略構成を示した図である。

【図１９】第１変更例に係る機器認証システムの内部構造を示したブロック図である。

【図２０】第２変更例に係る機器認証システムの概略構成を示した構成図である。

【図２１】第２変更例における複数の無線カードにある認証情報を１つの無線カードに統合した図を示したものである。

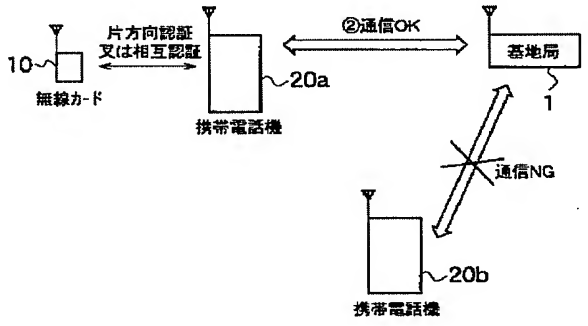
【図２２】第２変更例における無線カードで複数の電子機器と認証を行っていることを示した図である。

【図２３】従来におけるパスワードでの認証を示した図である。

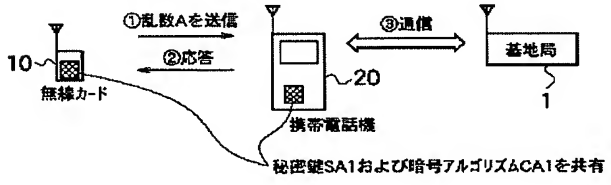
【符号の説明】

１…基地局、１０（１０ａ～１０ｃ）…無線カード、１１…ＣＰＵ、１２…ＲＯＭ、１３…ＲＡＭ、１３ａ…コード情報領域、１４…通信Ｉ／Ｆ、１４ａ…送信部、１４ｂ…受信部、１４ｃ…認証部、１５…表示部、１６…操作部、２０（２０ａ～２０ｃ）…携帯電話機／パーソナルコンピュータ／自動車、２１…ＣＰＵ、２１ａ…動作制御部、２１ｂ…検知部、２１ｃ…認識情報要求部、２１ｄ…設定部、２１ｅ…解除部、２２…ＲＯＭ、２３…ＲＡＭ、２３ａ…コード情報領域、２４…通信Ｉ／Ｆ、２４ａ…送信部、２４ｂ…受信部、２４ｃ…認証部、２５…表示部、２６…操作部、２７…電源部、３０…ホストシステム、３１…ＣＰＵ、３２…ＲＯＭ、３３…ＲＡＭ、３４…通信Ｉ／Ｆ、３５…記憶装置、３６…操作部、３７…表示部

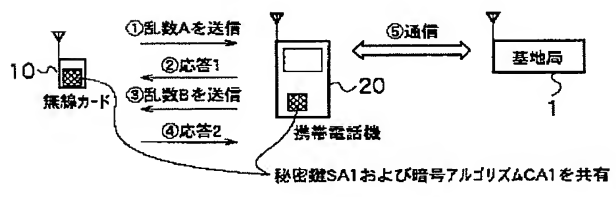
【図１】



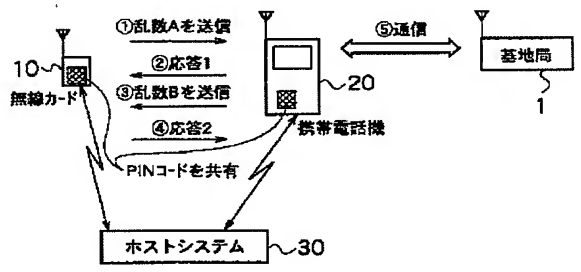
【図２】



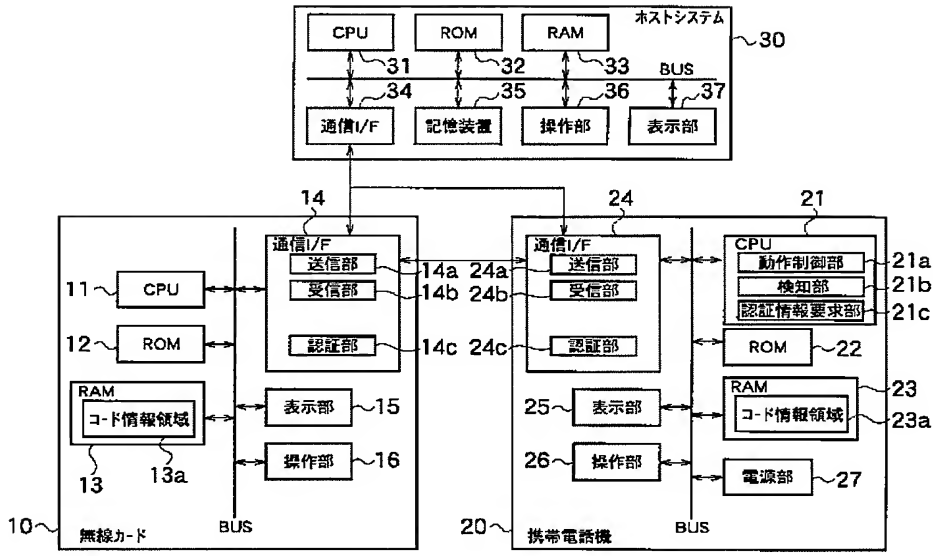
【図３】



【図４】



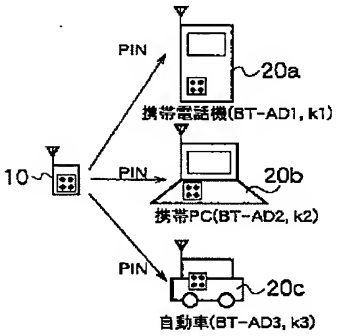
【図５】



【図６】

コード情報
乱数 （128ビット）
PINコード ,PINコード長
暗証番号 （例えば、"１２３４"）

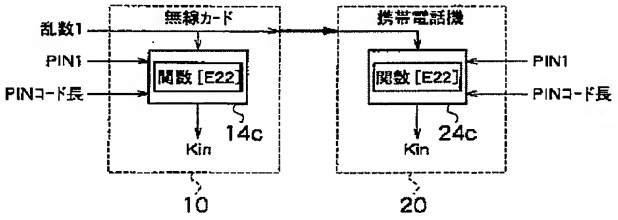
【図２２】



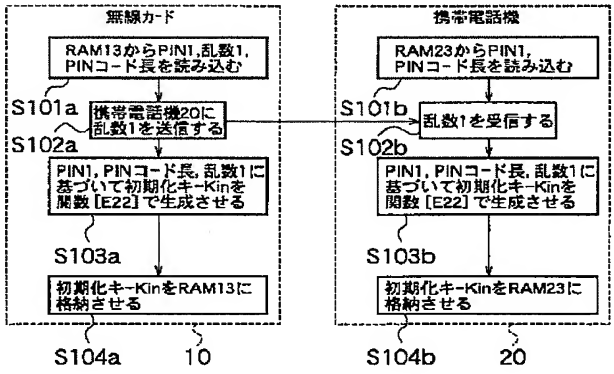
【図７】

端末機情報	
携帯端末機1	PIN1
携帯端末機2	PIN2
携帯端末機3	PIN3
・	・
・	・
携帯端末機n	PINn

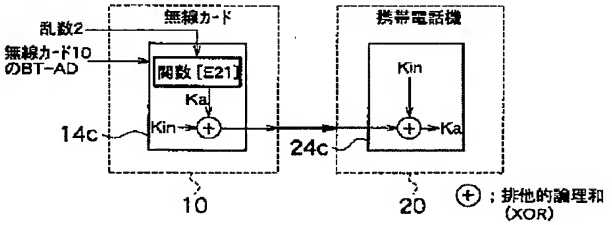
【図８】



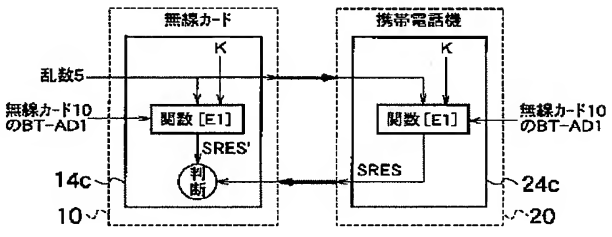
【図９】



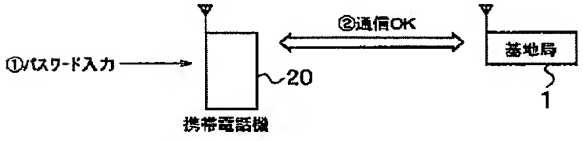
【図１０】



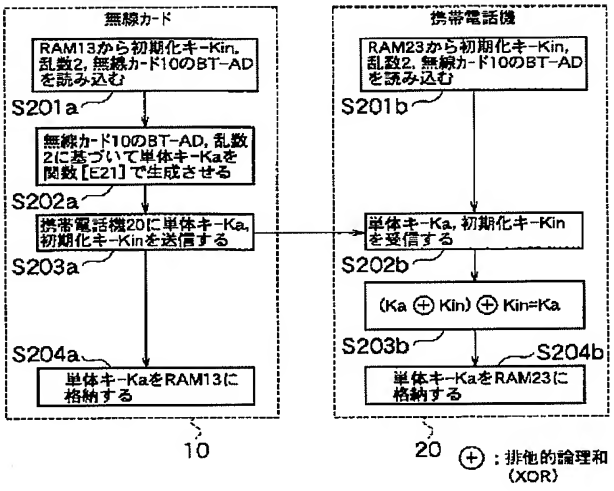
【図１４】



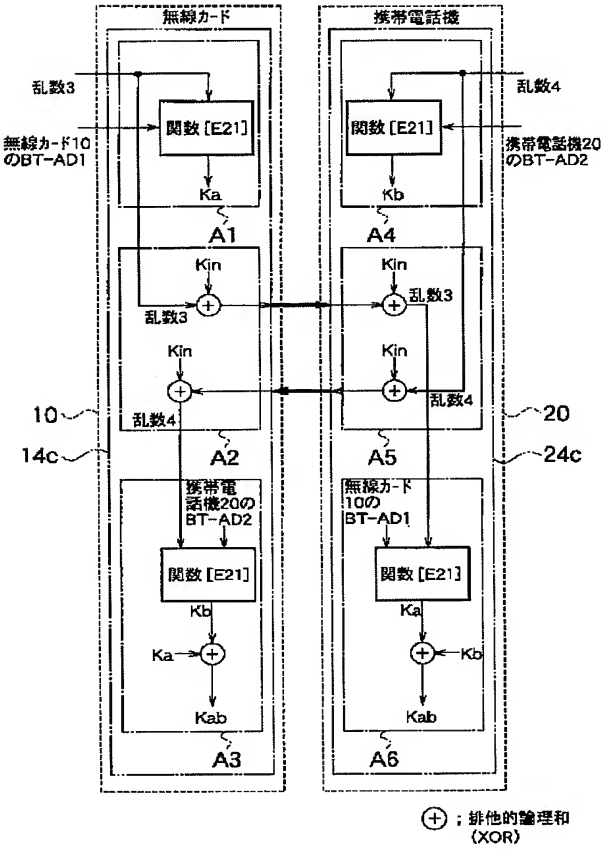
【図２３】



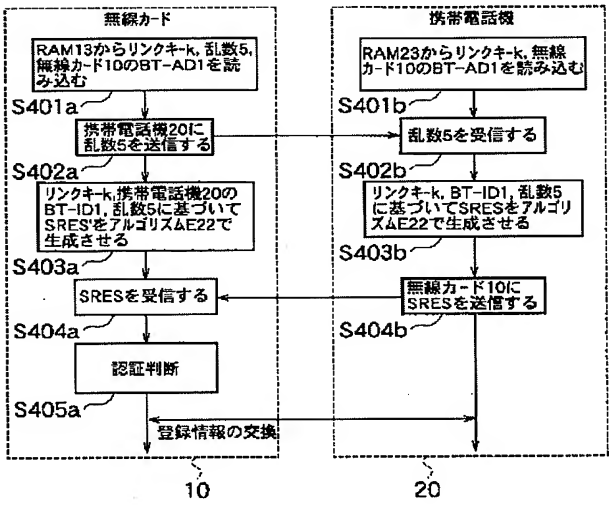
【図１１】



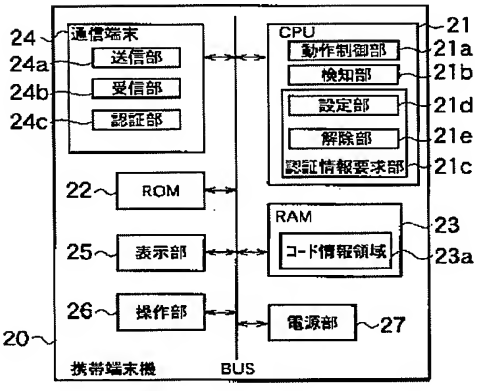
【図１２】



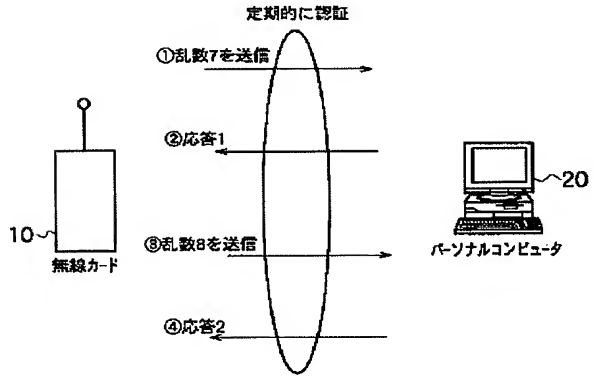
【図１５】



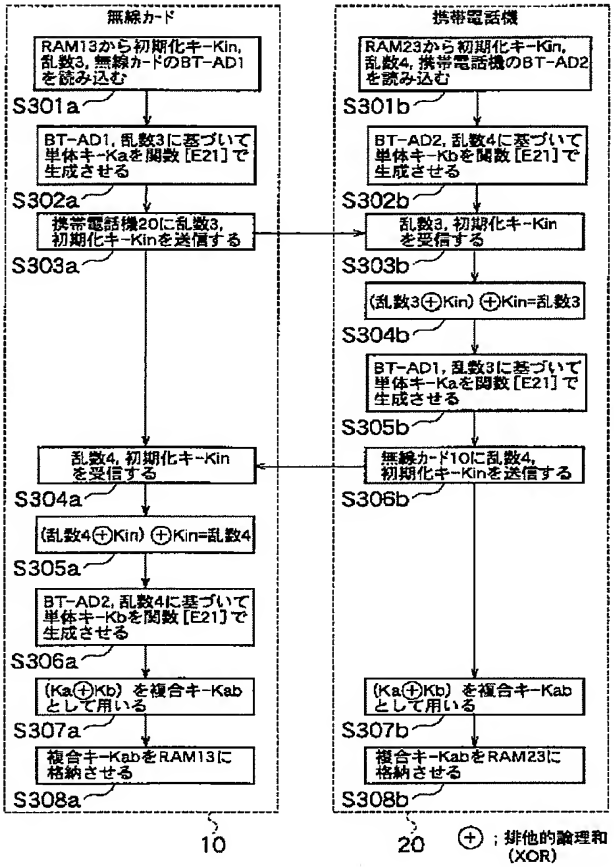
【図１８】



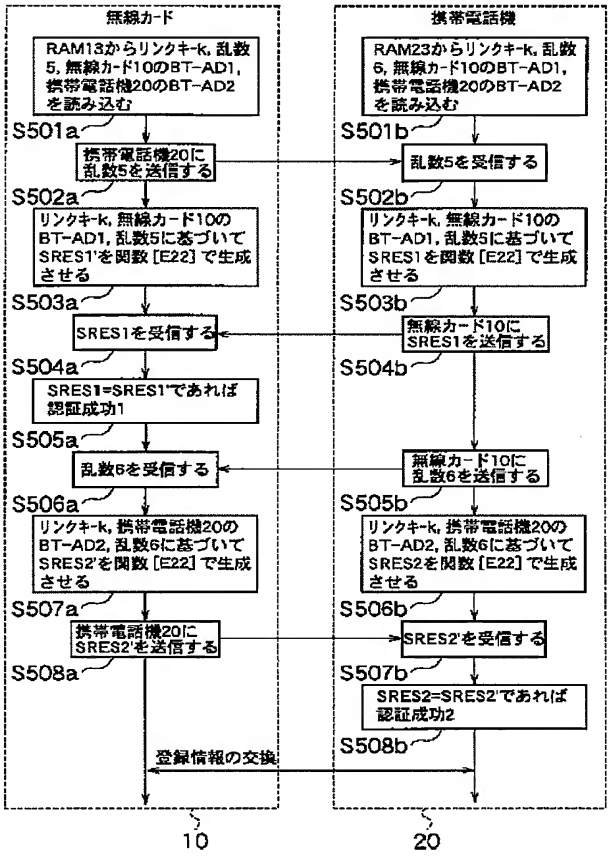
【図１９】



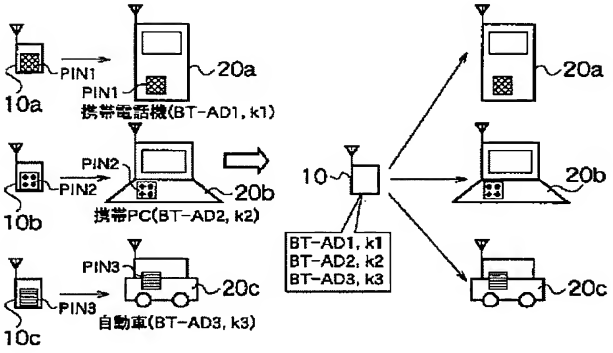
【図１３】



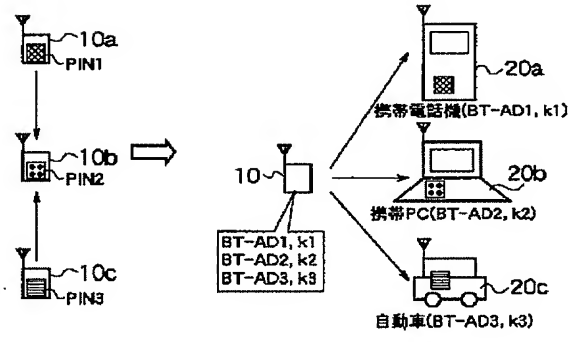
【図１６】



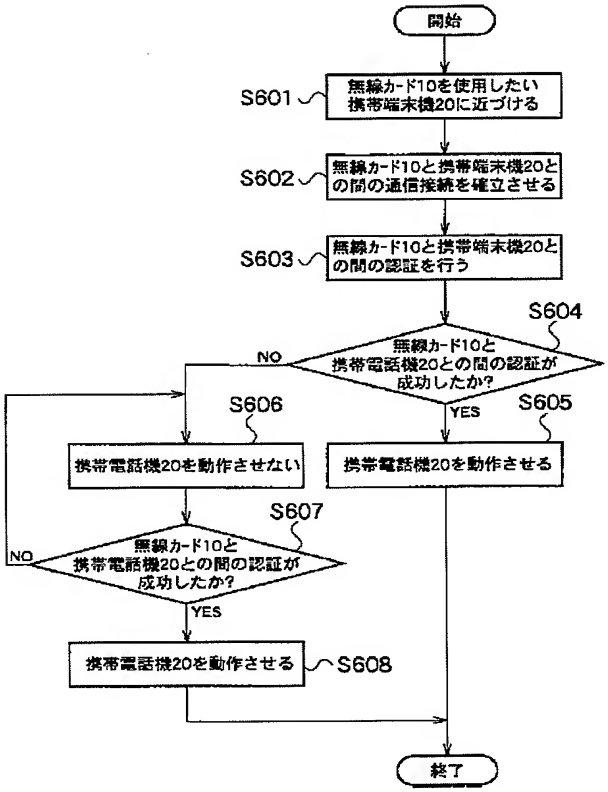
【図２０】



【図２１】



【図１７】



フロントページの続き

Ｆターム(参考)　5B085 AC12 AE09 AE12
5J104 AA04 AA07 KA02 KA04 KA15
NA02 PA02
5K067 AA32 BB04 CC04 CC08 CC10
DD17 EE02 EE10 FF23 HH21
HH22 HH23 HH36 KK13 KK15